UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/608,117 | 06/30/2000 | Kelan C. Silvester | 042390.P8691 | 1041 |

7590 02/02/2006

Walter T Kim
Blakely Sokoloff Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

| EXAMINER | |
|---|---|
| HOFFMAN, BRANDON S | |
| **ART UNIT** | **PAPER NUMBER** |
| 2136 | |

DATE MAILED: 02/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/608,117 | SILVESTER, KELAN C. | |
| | Examiner | Art Unit | |
| | Brandon S. Hoffman | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *16 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,2,4,5,7-19 and 21-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5,7-19 and 21-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1, 2, 4, 5, 7-19, and 21-26 are pending in this office action.

2. Applicant's arguments, filed November 16, 2005, have been fully considered but they are not persuasive.

### *Rejections*

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

### *Claim Rejections - 35 USC § 103*

4. Claims 1, 2, 4, 5, 7-19, 21, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rafizadeh (U.S. Patent No. 6, 401,183) in view of Puckette (U.S. Patent No. 6,385,721).

Regarding claim 1, Rafizadeh teaches a method comprising:

- Providing a partition on an Integrated Device Electronics (IDE) storage device of a computer system, wherein said partition is invisible to an operating system of the computer system unless the partition is unlocked (fig. 3 and col. 10, lines 21-26);

- Providing a software task having knowledge about a proper handshake to unlock the partition such that the partition that was previously invisible to the operating system becomes visible to the operating system (fig. 1, ref. num 5, fig. 13, ref. num 316 and col. 8, lines 53-66); and
- Unlocking the partition in response to an unlock request received from the software task **after the software task performs** the handshake to unlock the partition, wherein the partition is visible to the operating system when unlocked (col. 8, lines 53-55).

Rafizadeh does not teach **establishing a proper unlock handshake between the software task and an IDE controller for controlling the storage device**.

Puckette teaches **establishing a proper unlock handshake between the software task and an IDE controller for controlling the storage device** (col. 7, lines 47-58).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine unlocking the partition by establishing a handshake between the software task and the IDE controller, as taught by Puckette, with the method of Rafizadeh. It would have been obvious for such modifications because the BIOS, which can be stored in a secure hibernation partition, can be updated securely by

providing the proper credentials to unlock the secure partition (see col. 7, lines 47-58 of Puckette).

Regarding claim 2, the combination of Rafizadeh as modified by Puckette teaches wherein the storage device is a hard disk drive having an IDE disk controller (see col. 1, lines 13-17 of Rafizadeh).

Regarding claim 4, the combination of Rafizadeh as modified by Puckette teaches wherein the software task requests a master token from the IDE controller when the computer system is first turned on and the unlock handshake between the software task and the IDE controller is established by passing the master token back to the IDE controller as a parameter (see col. 7, line 59 through col. 8, line 7 of Puckette).

Regarding claim 5, the combination of Rafizadeh as modified by Puckette teaches wherein the software task requests a master token from the disk controller when the computer system is first turned on, said master token is used by the software task to initiate the proper handshake to unlock the partition (see col. 7, line 59 through col. 8, line 7 of Puckette).

Regarding claim 7, the combination of Rafizadeh as modified by Puckette teaches wherein the software receives a usage token from an IDE controller when the partition is unlocked and the access handshake between the software and the IDE

controller is established by passing the usage token back to the IDE controller as a parameter (see col. 7, line 59 through col. 8, line 7 of Puckette).

Regarding claim 8, the combination of Rafizadeh as modified by Puckette teaches further comprising locking the partition in response to a lock request received from a software having knowledge about a proper handshake for locking the partition (see fig. 13, ref. num 316, col. 2, lines 47-48, and col. 8, lines 53-66 of Rafizadeh).

Regarding claim 9, the combination of Rafizadeh as modified by Puckette teaches further comprising providing a standard partition on the storage device (see fig. 14, ref. num 102-112 of Rafizadeh), wherein said standard partition is always visible to the operating system and generally accessible to other software (see col. 1, lines 13-17 of Rafizadeh).

Regarding claim 10, Rafizadeh teaches a machine-readable medium that provides instructions, which when executed by a set of processors, causes said set of processors to perform operations comprising:

- Receiving an open request from a software to access a secure-private partition on an IDE hard drive of a computer system (col. 8, lines 53-55);
- Requesting unlocking of the secure-private partition in response to the validation of the open request received from the software (fig. 13, ref. num 316 and col. 8, lines 53-66);

- Unlocking the secure-private partition in response to the unlocking request such that the partition that was previously invisible to an operating system becomes visible to the operating system (col. 8, lines 53-55); and
- Preventing an access to the secure-private partition when the secure-private partition is unlocked unless the access is requested by a software having knowledge about a proper access handshake for accessing the secure-private partition (col. 9, lines 35-61).

Rafizadeh does not teach validating the open request received from the software.

Puckette teaches validating the open request received from the software (col. 8, lines 14-24).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine validating the open request received from the software, as taught by Puckette, with the medium of Rafizadeh. It would have been obvious for such modifications because password validation, or other means of validation, protects against malicious code from randomly "guessing" the appropriate validation parameters.

Regarding claim 11, the combination of Rafizadeh as modified by Puckette teaches wherein the operations further comprise requesting locking of the

secure-private partition in response to a close request received from the software (see fig. 13, ref. num 316 and col. 8, lines 53-66 of Rafizadeh).

Regarding claim 12, the combination of Rafizadeh as modified by Puckette teaches wherein the requesting of the unlocking of the secure partition further comprises: requesting a master token from an IDE controller when the computer system is turned on; storing the master token in a secure storage location; retrieving the master token from the secure storage location when an access to a secure-private partition is needed; and passing the master token as a parameter to the IDE controller (col. 7, line 59 through col. 8, line 7).

Regarding claim 13, the combination of Rafizadeh as modified by Puckette teaches wherein the operations further comprise requesting an access to the secure-private partition in response to an access request received from the software (see col. 7, lines 47-58 of Puckette, BIOS is the software).

Regarding claim 14, the combination of Rafizadeh as modified by Puckette teaches wherein the requesting of the access to the secure partition further comprises:

- Receiving a usage token (see col. 8, lines 2-7 of Puckette); and
- Passing the usage token to the IDE controller to gain an access to the secure partition (see col. 8, lines 2-7 of Puckette).

Regarding claim 15, the combination of Rafizadeh as modified by Puckette teaches wherein the request from the software to access the secure-private partition is received by a privacy gatekeeper which prescreens the request to determine if the software has an authorization to access the secure-private partition (see fig. 2, ref. num 56 and col. 8, lines 14-24 of Puckette).

Regarding claim 16, Rafizadeh teaches a system comprising:

- A storage device having a storage controller (col. 1, lines 13-17),
    - Said storage device having at least one secure-private partition (fig. 3, ref. num 14),
    - Wherein said secure-private partition is selectively in one of locked and unlocked modes, wherein said secure-private partition is invisible to an operating system when it is locked and the secure-private partition is visible to the operating system when it is unlocked (col. 10, lines 21-26);
- An IDE controller operatively coupled to the storage controller (col. 1, lines 13-17); and
- A security/privacy software task operatively coupled to the IDE controller (fig. 1, ref. num 5),
    - Wherein an unlock request is initiated to unlock the secure-private partition in response to a valid unlock handshake, and initiating a lock request to lock the secure-private partition in response to a valid lock handshake (fig. 13, ref. num 316 and col. 8, lines 53-66).

Rafizadeh does not specifically teach the IDE controller initiating an unlock/lock request in response to an unlock/lock request between the IDE controller and the software task.

Puckette teaches the IDE controller initiating an unlock/lock request in response to an unlock/lock request between the IDE controller and the software task (col. 7, line 47 through col. 8, line 7).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the IDE controller initiating an unlock/lock request in response to an unlock/lock request between the IDE controller and the software task, as taught by Puckette, with the system of Rafizadeh. It would have been obvious for such modifications because the BIOS, which can be stored in a secure hibernation partition, can be updated securely by providing the proper credentials to unlock/lock the secure partition (see col. 7, lines 47-58 of Puckette) and the token used for gaining access provides encryption/decryption capabilities for the data residing the on the secure hibernation partition (see col. 8, lines 2-7 of Puckette).

Regarding claim 17, the combination of Rafizadeh as modified by Puckette teaches wherein the security/privacy software task requests a master token from the IDE controller when the system is turned on and sends the master token to the IDE

controller as a parameter when making a request to the IDE controller to unlock the secure-private partition (see col. 7, line 59 through col. 8, line 7 of Puckette).

Regarding claim 18, the combination of Rafizadeh as modified by Puckette teaches further comprising a requesting software and a privacy gatekeeper which acts as a gatekeeper to the security/privacy software task (see fig. 2, ref. num 56 of Puckette), wherein when the requesting software makes a request to access the secure-private partition, the privacy gatekeeper prescreens the request to determine if the requesting software has an authorization to access the secure-private partition (see fig. 2, ref. num 56 and col. 8, lines 14-24 of Puckette).

Regarding claim 19, the combination of Rafizadeh as modified by Puckette teaches wherein the IDE controller allows an access to said at least one secure-private partition only when a valid access handshake is established between the requesting software and the IDE controller (see col. 8, lines 14-24 of Puckette).

Regarding claim 21, the combination of Rafizadeh as modified by Puckette teaches preventing an access to the partition when the partition is unlocked unless the access is requested by a software having knowledge about a proper access handshake for accessing the partition (see col. 9, lines 35-61 of Rafizadeh).

Regarding claim 22, the combination of Rafizadeh as modified by Puckette teaches wherein the IDE controller generates and returns a usage token to the requesting software once the secure-private partition is unlocked (see col. 7, line 59 through col. 8, line 7 of Puckette), wherein the access handshake is established between the IDE controller and the requesting software when the IDE controller validates the usage token passed back by the requesting software (see col. 8, lines 14-24 of Puckette).

Regarding claim 23, Rafizadeh teaches a method comprising:

- Partitioning a hard disk into a standard partition and a secure-private partition (SPP), the SPP operable in a locked mode and an unlocked mode (col. 10, lines 54-63);
- Switching the SPP from the locked mode to the unlocked mode in response to a handshake (fig. 13, ref. num 316 and col. 8, lines 53-66);
- Receiving at least one read/write request from a requesting software program (col. 4, lines 46-49); and
- Switching the SPP from the unlocked mode to the locked mode in response to a close request (fig. 13, ref. num 316, col. 2, lines 47-48, and col. 8, lines 53-66).

Rafizadeh does not teach wherein each of the at least one read/write requests is accompanied by a usage token (col. 7, line 59 through col. 8, line 7).

Puckette teaches wherein each of the at least one read/write requests is accompanied by a usage token (col. 7, line 59 through col. 8, line 7).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine accompanying each read/write request with a usage token, as taught by Puckette, with the method of Rafizadeh. It would have been obvious for such modifications because the BIOS, which can be stored in a secure hibernation partition, can be updated securely by providing the proper credentials to unlock/lock the secure partition (see col. 7, lines 47-58 of Puckette) and the token used for gaining access provides encryption/decryption capabilities for the data residing the on the secure hibernation partition (see col. 8, lines 2-7 of Puckette).

Regarding claim 24, the combination of Rafizadeh as modified by Puckette teaches wherein the handshake comprises:

- Receiving a secure token from a requesting software program (see col. 8, lines 2-7 of Puckette);
- Verifying the secure token (see col. 8, lines 14-24 of Puckette); and
- Returning a usage token to the requesting software program (see col. 7, line 59 through col. 8, line 7 of Puckette).

Regarding claim 25, the combination of Rafizadeh as modified by Puckette teaches further comprising validating the usage token received with a read/write

request, and, if the token is valid, performing the request (see col. 8, lines 14-24 of Puckette); or if the token is invalid, denying the request (see col. 9, lines 35-61 of Rafizadeh).

Regarding claim 26, the combination of Rafizadeh as modified by Puckette teaches further comprising generating a new usage token after the read/write request; and returning the new usage token to the requesting software program (see col. 7, line 59 through col. 8, line 7 of Puckette).

***Response to Arguments***

5. Applicant amends claim 1.

6. Applicant argues:

   a. The references do not teach wherein the unlocking of the partition is initiated by establishing a proper unlock handshake between the software task and an IDE controller for the storage device (page 8, last paragraph through page 9, second paragraph and page 10, third paragraph).

   b. The references do not teach validating an open request received from a software program (page 9, last paragraph through page 10, first paragraph).

Regarding argument (a), examiner disagrees with applicant. In the applied art (Puckette), the software task is the BIOS and the IDE controller is the mass storage device. The BIOS communicates with the mass storage device to establish a way for

the BIOS to gain access to the hidden hibernation partition for the use of the content stored therein. A proper unlock handshake in Puckette is simply the steps necessary to allow the BIOS access to the hibernation partition, while blocking access to all other software applications as well as the user.

Regarding argument (b), examiner disagrees with applicant. First, applicant stated that the request in Puckette came for a user, not software. Examiner would like to point out that the request to unlock the hibernation partition is controlled by the BIOS gaining access to the hibernation partition. BIOS is a software task. Second, the request to open/unlock the partition is validated in that the BIOS, and only the BIOS, is able to open/unlock the hidden partition. It is apparent that validation takes place, or else any software application (viruses included) would be able to access the hidden partition.

***Conclusion***

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

Primary Examiner
AU2131
1/31/06